A NEW PROOF OF SYLOW'S THEOREM.

By G. A. Miller.

The main part of Sylow's theorem relates to the fact that a necessary and sufficient condition that any group G of finite order g contain a subgroup whose order is p^α, p being a prime number, is that g is divisible by p^α. In particular, if p^α is the highest power of p which divides g, then G contains at least one subgroup of order p^α. This theorem was first proved by L. Sylow in the Mathematische Annalen, volume 5 (1872), page 584. Among the later proofs those by A. Capelli, E. Netto, and G. Frobenius are most noteworthy from the standpoint of originality and simplicity. The present writer has recently pointed out* that a simple proof of this theorem can also be obtained by modifying only slightly the method employed by A. Cauchy to prove the special but fundamental case that G contains a subgroup of order p whenever g is divisible by p.

Notwithstanding these various known proofs it seems desirable to direct attention to the following very elementary proof, especially since this proof follows almost directly from an elementary theorem which is of interest on its own account. This theorem may be stated as follows: *The number of the substitutions of degree p^β and of order p in the symmetric group of degree n is prime to p whenever p^β is the highest power of p which does not exceed n.*

For simplicity we shall first consider the case when $n = p^\beta$ in proving this theorem. It is evident that the subgroup of the symmetric group of degree p^β which is composed of all the substitutions of this symmetric group which are commutative with a substitution s of degree p^β and of order p is of order

$$p^{p^{\beta-1}} \cdot p^{\beta-1}!.$$

In fact, s is composed of $p^{\beta-1}$ cycles and these cycles are permuted according to the symmetric group of degree $p^{\beta-1}$ under the group which transforms s into itself.

All the factors of $p^\beta!$ which are divisible by p are evidently contained in the series

$$p,\ 2p,\ 3p,\ \cdots,\ p^{\beta-1} \cdot p.$$

Hence the order of this group involves the highest power of p which divides

* G. A. Miller, Bulletin of the American Mathematical Society, vol. 16 (1910), p. 511.

$p^\beta!$ and hence the number of conjugates of s under the symmetric group of degree p^β is prime to p.

Having proved the theorem in question when $n = p^\beta$ it is not difficult to prove it in general. In fact, the number of the substitutions which are similar to s and which are contained in the symmetric group of degree $p^\beta + k$ is evidently equal to

$$\frac{N(p^\beta + 1)(p^\beta + 2) \cdots (p^\beta + k)}{k!},$$

where N represents the number of these substitutions in the symmetric group of degree p^β. As $p^\beta + k$ and k are divisible by the same power of p whenever $p^\beta < p^\beta + k < p^{\beta+1}$, the theorem in question has been proved.

To prove Sylow's theorem by means of the theorem which has just been established let G be any group whose order g is divisible by p^α but not by $p^{\alpha+1}$, and represent G as a regular substitution group. Suppose that p^β is the highest power of p which is less than g, since the case when g is a power of p does not require consideration, and consider all the possible substitutions on the g letters of G which are of degree p^β and of order p. Since G is transitive, it cannot transform any of these substitutions into itself. It must therefore transform all of them into complete sets of conjugates under G such that each of these sets is composed of more than one substitution. As the total number of these substitutions is prime to p, at least one of these sets of conjugates involves a number m of substitutions, where m is prime to p.

Each of these m substitutions is transformed into itself by a subgroup of G whose order is g/m, where $m > 1$. Hence G contains a subgroup whose order is divisible by p^α. If this subgroup is of order p^α, our theorem is established. If it is not of this order, we have reduced our problem to that of a smaller group whose order is divisible by p^α. In case Sylow's theorem were not universally true it would clearly be possible to find a smallest group G for which it would not be satisfied. As the preceding considerations establish the fact that such a smallest group does not exist these considerations constitute a proof of Sylow's theorem.

The main elements which enter into the above proof, besides the given theorem, are the facts that every group of finite order can be represented as a regular substitution group, and that the total number of substitutions of a group which transform into itself any one of a system of more than one conjugates under this group constitute a subgroup whose index under this group is equal to the number of these conjugates. Both of these very elementary theorems were known long before Sylow's theorem was

first proved. As the proof of the italicized theorem is also based upon very elementary considerations the present proof is elementary as well as brief. It is not affected by the fact that G may be abelian or non-abelian.

For the sake of completeness it may be desirable to add that the italicized theorem mentioned above is a special case of the following: *A necessary and sufficient condition that the number of the substitutions of degree* p^β *and of order* p *in the symmetric group of degree* n *is divisible by* p *is that the coefficient of* p^β *is zero if* n *is written in the form* $a_0p^m + a_1p^{m-1} + \cdots + a_m$, *where the coefficients* $a_0, a_1, \cdots, a_m$ *are integers less than* p *and either positive or zero.* The proof of this theorem is similar to that of the special case given above. In the proof of Sylow's theorem we can evidently select for s any substitution of degree p^β and of order p such that the number of all its conjugates under the symmetric group of degree n is prime to p.

UNIVERSITY OF ILLINOIS.